

REMARKS

STATUS OF CLAIMS

Claims 1-7, 11, and 13-23 have been amended.

Claims 26-31 have been added.

No claims have been cancelled or withdrawn.

Claims 1-7, 11, and 13-31 are currently pending in the application.

INTERVIEW SUMMARY

The Applicant thanks the Examiner for the telephone interview conducted on April 8, 2005. The interview was between Examiner Justin Darrow and the applicant's attorney, Craig G. Holmes. During the interview, the status of the Information Disclosure Statement (IDS) and Form 1449 submitted on April 19, 2005 and resubmitted on September 15, 2004 with the payment of the Issue Fee were discussed. As requested by Examiner Darrow, a listing of the IDS's and Form 1449's that have been submitted are provided below, along with an indication of which initialed Form 1449's have been returned to the Applicant.

During the interview, the allowability of Claims 1-7, 11, and 13-24 over the cited prior art reference of *Waldvogel* were discussed. In particular, the step of Claim 1 featuring "receiving a new group session key...from a local multicast proxy service node that has received the original group session key through periodic replication of the first directory" was discussed with respect to paragraphs [0056] and [0057] of *Waldvogel*. In addition, the "second directory" of Claim 2 was discussed with respect to paragraph [0061] of *Waldvogel*. However, no agreement was reached as to the allowability of the claims.

INFORMATION DISCLOSURE STATEMENTS AND FORM 1449'S

The Applicant thanks the Examiner for returning the initialed and dated Form 1449 for the Information Disclosure Statement (IDS) that was filed on September 8, 2004. However, the Applicant has still not received the initialed and dated Form 1449 for the IDS that was filed on April 19, 2004 and which was the subject of the Petition to Defer Issue that was submitted with the payment of the Issue Fee on September 15, 2004. The Petition to Defer

Issue included a copy of the IDS filed on April 19, 2004, including a copy of the postcard that was received from the Office showing that the IDS was received by the Office on April 22, 2004.

The Examiner explained during the interview that the seven month delay since the copy of the April 19, 2004 IDS was supplied on September 15, 2004 is not an unusually long delay to be scanned into the Image File Wrapper (IFW) system and that that copy of the April 19, 2004 should make its way into the IFW system in the near future. Thus, a second copy of the April 19, 2004 IDS is not being submitted herein.

As requested by the Examiner during the Interview, the Applicant is providing the following list of IDS's with Form 1449's that have been submitted in this application, along with an indication of whether the Form 1449 has been returned to the Applicant.

Mailing Date of IDS	Date IDS Received by the USPTO	Form 1449 Returned?
December 27, 2000	January 3, 2001	Yes – with OA dated 1/16/04
April 19, 2004	April 22, 2004	<u>No</u> – subject of Petition to Defer Issue filed 9/15/04
September 8, 2004	September 13, 2004	Yes – with FOA dated 2/22/05
November 2, 2004	November 5, 2004	No – filed under 37 CFR 1.97(i)

Note that the IDS that was sent on November 2, 2004 was submitted under 37 CFR 1.97(i) for inclusion in the file but which was not to be considered. However, the contents of that IDS is now being resubmitted in a new IDS under 37 CFR 1.97(b) along with this submission for consideration by the Examiner.

Therefore, the Applicant respectfully requests that the Examiner return the initialed and dated Form 1449's from both the April 19, 2004 IDS and from the IDS being filed concurrently with this submission (which was previously filed on November 2, 2004, for inclusion in the file but not to be considered). If a second copy of the April 19, 2004 IDS is required, the Applicant respectfully requests that the Examiner contact the Applicant's attorney, Craig G. Holmes at (408) 414-1207 to request that a second copy of the April 19, 2004 IDS be provided to the Office.

SUMMARY OF THE REJECTIONS/OBJECTIONS

Claims 1-7, 11, and 13-14 have been rejected under 35 U.S.C. § 102(a) as allegedly anticipated by European Patent Application No. EP 0 952 718 A2 by Sun Microsystems, Inc., and listing as inventors Marcel Waldvogel et al. (“*Waldvogel*”). Claim 25 has been objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. The rejections are respectfully traversed.

A. CLAIM 1

As amended above, Claim 1 features:

“A method for communicating a session key from a first multicast proxy service node of a secure multicast group to a plurality of other multicast proxy service nodes of the secure multicast group in a communication network, wherein each of the multicast proxy service nodes is capable of establishing multicast communication and serving as a key distribution center, the method comprising the steps of:

creating and storing an original group session key associated with the secure multicast group *in a first directory that is based on the Lightweight Directory Access Protocol (LDAP) directory standard;*

authenticating the first multicast proxy service node with a subset of the multicast proxy service nodes that are affected by an addition of the first multicast proxy service node to the secure multicast group, *based on the original group session key stored in the first directory that is based on the LDAP directory standard;*

receiving a plurality of private keys from the subset of the multicast proxy service nodes;

receiving a new group session key for the secure multicast group, for use after addition of the first multicast proxy service node, *from a local multicast proxy service node that has received the original group session key through periodic replication of the first directory that is based on the LDAP directory standard;*

communicating the new group session key to the first multicast proxy service node;
and
communicating a message to the subset of the multicast proxy service nodes that
causes the subset of the multicast proxy service nodes to update their private
keys.” (emphasis added).

Thus, Claim 1 features “storing an original group session key associated with the secure multicast group *in a first directory that is based on the Lightweight Directory Access Protocol (LDAP) directory standard*” and “a local multicast proxy service node that has received the original group session key through periodic *replication of the first directory that is based on the LDAP directory standard...*” In other words, in the approach of Claim 1, the local multicast proxy service node obtains the group session key via replication of a directory that is based on the LDAP directory standard.

For example, an embodiment in the Application on page 9, lines 13-18 is described as follows: “Because keys as well as key version information are housed in the directory, multicast security can be achieved over any number of network domains across the entire enterprise. **Key information is stored in**, and the logical tree is supported by, **a directory service. Replication of the directory accomplishes distribution of keys.** Event service nodes may obtain current key information from a local copy of the replicated directory.” (Emphasis added.)

As further described in the Application on page 15, lines 2-13, a directory can be implemented based on the Microsoft Active Directory, which in turn is based on the Lightweight Directory Access Protocol (LDAP) directory standard. LDAP is based on the International Telecommunications Union (ITU) X.500 standard that employs a distributed approach of storing information locally in Directory System Agents (DSAs). The details of LDAP are set forth in RFC 1777 and RFC 2251.

As explained in the Application, in “general, a directory creates active associations among users, applications, a network, and network devices. A directory is a logically centralized, highly distributed data repository” that can be accessed by applications. (Application, page 14, lines 19-21.) “The distributed nature of directories is achieved by replicating data across multiple directory servers, which are strategically located throughout

the network...Directories can represent network elements, services, and policies to enable each of network administration and security.” (Application, page 14, lines 21-25.) When a group session key is generated, the group session key can be stored in a local domain, following which directory replication occurs such that a common group session key can be obtained from a local copy of the directory, and as a result, a large number or block of keys can be distributed using directory replication. (Application, page 30, lines 10-16.)

Thus, the amendment to Claim 1 to clarify that the first directory is based on the LDAP directory standard is fully supported by the specification as filed. No new matter is introduced. Note that in addition to the amendments to Claim 1 to clarify that the first directory is based on the LDAP directory standard, similar changes are made to Claims 2-7, 11, and 13-23 and are reflected in Claims 26-31 to clarify that both the first directory and the second directory are based on the LDAP directory standard. As explained above, these amendments are fully supported by the specification as filed. No new matter is introduced.

In contrast to Claim 1, *Waldvogel* discloses an approach for multicasting that provides secure multi-destination communications over an unsecured communication channel in a scalable manner for highly dynamic groups of arbitrary size with minimal computation and storage requirements required of the participants. (Paragraphs [0018], [0022], and [0023].) *Waldvogel* incorporates the use of a group key manager database 300, as illustrated in Figure 3, for implementing key control group 107 or 117 as either a centralized database or a distributed database. (Paragraph [0049].) Key control group 107 and key control group 117 are each a virtual subgroup of participants defined by shared keying information and linked by a multicast or broadcast. (Paragraphs [0036], [0038].)

Note that group key manager database 300 and key control groups 107, 117 are involved in key management for the multicast or broadcast, but none of group key manager database 300 or key control groups 107, 117 are described in *Waldvogel* as being involved in performing the functions of a directory as discussed above. In addition, the Applicant has been unable to locate any mention in *Waldvogel* of the LDAP directory standard, little less a “first directory that is based on the LDAP directory standard,” as featured in Claim 1.

In addition, the Final Office Action states that *Waldvogel* discloses “creating and storing an original group session key associated with the secure multicast group in a first directory (see ¶ [0042]; figure 1a, item 108; figure 2, item 203; generating a traffic encryption

key (TEK) for encrypting messages generated in a participant multicast application; see ¶¶ [0049] – [0050]; figure 3, item 300; and holding the current traffic encryption key (TEK) in a group key manager database.” Thus, Final Office Action is equating the “group key manager database” 300 of Figure 3 of *Waldvogel* with the first directory of Claim 1.

While the Application describes that a directory server can be implemented using a database and that one or more master copies of the database are maintained along with a number of replicas, such as the Microsoft Active Directory that is based on the LDAP directory standard (Application, age 15, lines 2-10), Claim 1 does not recite a “database.” Rather, Claim 1 recites a “directory” and thus even if the “first directory” of Claim 1 is implemented using a database, the “first directory” also functions as a “**directory**.” However, the group key manager database 300 of *Waldvogel* is described as merely storing key information, and there is nothing in *Waldvogel* that discloses or suggests that the group key manager database can also serve as a “directory.” Thus, the group key manager database of *Waldvogel* is not a “directory” as featured in Claim 1, little less a directory that is based on the LDAP standard, as featured in Claim 1.

In addition, the Final Office Action states that *Waldvogel* discloses “receiving a new group session key...from a local multicast proxy service node that has received the original group session key (see ¶ [0059]; figure 1a, items 101 and 108; from a first participant that has the ad hoc traffic encryption key TEK from the creation of the group); through periodic replication of the first directory (see ¶¶ [0056] – [0057]; periodically changing keying material and revision numbers causing keys to change equivalent to periodic replication of the group key database)...” However, the Applicant disagrees that periodically changing keying material and revision numbers so that the participants generate new keys is equivalent to periodic replication of a directory, as featured in Claim 1, for at least the following reasons.

First, assuming that the group key database is a “directory” as featured in Claim 1 (which the Applicant respectfully submits is not the case, as explained above), Claim 1 expressly recites replication of the “directory” and not the replication of a key that may be stored in the directory. Because the Final Office Action equates the group key manager database with the directory, the group key database of *Waldvogel* would need to be replicated for Claim 1 to read on the disclosure of *Waldvogel*. However, *Waldvogel* merely discloses that the group keys are generated by each participant and the group key manager, and that the

group key is stored in the group key database. Nowhere in *Waldvogel* is there any disclosure or suggestion that the group key manager database is ever replicated.

Second, *Waldvogel* describes the generation of new keying material by each participant based on an increased revision number, “without the need for communicating the new keying material itself” because the “system-defined one-way function...is known and identical among the group key manager 108 (or key manager 118) and each participant key manager component 109 (or 119).” (Paragraph [0056].) Thus, *Waldvogel* clearly and unambiguously distinguishes the communication of a key revision number from the communication of a key, with the key being separately generated by each participant based on the key revision number that is received. Yet Claim 1 expressly features a “node that has *received* the original group session *key*...” Thus, receiving a “revision number” as disclosed in *Waldvogel* is not the same as receiving a group session *key* as featured in Claim 1.

Third, while *Waldvogel* discloses that the group key manager database includes session keys and that the group key manager 108 or 118 and each participant in the multicast can generate a new session key based on a revision number that is received, Claim 1 expressly features “replication of the first directory.” This means that the directory itself is replicated in addition to the contents of the directory. This is fundamentally different than the participants generating the same key that happens to also be included in the group key manager database, as disclosed in *Waldvogel*.

There is nothing in *Waldvogel* that discloses or suggests that the group key manager database itself and that the information stored in the database are being “replicated” by the participants of the multicast. Therefore, changing key revision numbers so that participants generate new keys as disclosed in *Waldvogel* is not “equivalent” to “periodic replication of the first directory,” little less “periodic replication of the first directory that is based on the LDAP directory standard,” as featured in Claim 1.

Because *Waldvogel* fails to disclose, teach, suggest, or in any way render obvious “storing an original group session key ... in a *first directory that is based on the Lightweight Directory Access Protocol (LDAP) directory standard*” and “a local multicast proxy service node that has received the original group session key through periodic *replication of the first directory that is based on the LDAP directory standard*...” as featured in Claim 1, for at

least the reasons stated above, Claim 1 is allowable over the art of record and is in condition for allowance.

B. CLAIMS 7, 11, 13, AND 26

Claims 7, 11, 13, and 26 contain features that are similar to those described above with respect to Claim 1. In particular both Claims 7 and 13 feature “storing an original group session key associated with the secure multicast group *in a first directory that is based on the Lightweight Directory Access Protocol (LDAP) directory standard*” and “a local multicast proxy service node that has received the original group session key through periodic *replication of the first directory that is based on the LDAP directory standard...*,” both of which are the same as in Claim 1.

Furthermore, Claim 11 features “one of the multicast proxy service nodes generates a first group session key...and distributes the first group session key to other multicast proxy service nodes in the secure multicast or broadcast group using *directory replication of a directory that is based on the Lightweight Directory Access Protocol (LDAP) directory standard,*” which is similar to Claim 1.

Finally, Claim 26 features “means for storing an original group session key associated with the secure multicast group *in a first directory that is based on the Lightweight Directory Access Protocol (LDAP) directory standard*” and “a local multicast proxy service node that has received the original group session key through periodic *replication of the first directory that is based on the LDAP directory standard...*,” which is similar to Claim 1.

Therefore, based on at least the reasons stated above with respect to Claim 1, Claims 7, 11, 13, and 26 are allowable over the art of record and are in condition for allowance.

C. CLAIMS 2-6, 14-18, 19-23, 24-25, AND 27-31

Claims 2-6, 14-18, 19-23, 24-25, and 27-31 are dependent upon Claims 1, 13, 7, 11, and 26, respectively, and thus include each and every feature of the corresponding independent claims. Each of Claims 2-6, 14-18, 19-23, 24-25, and 27-31 is therefore allowable for the reasons given above for Claims 1, 13, 7, 11, and 26. In addition, each of Claims 2-6, 14-18, 19-23, 24-25, and 27-31 introduces one or more additional limitations that

independently render it patentable. However, due to the fundamental differences already identified and in order to expedite the positive resolution of this case, a separate discussion of those limitations is not included at this time. Therefore, Claims 2-6, 14-18, 19-23, 24-25, and 27-31 are allowable for the reasons given above with respect to Claims 1, 13, 7, 11, and 26.

CONCLUSION

The Applicant believes that all issues raised in the Final Office Action have been addressed and that allowance of the pending claims is appropriate. After entry of the amendments, further examination on the merits is respectfully requested.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.


To the extent necessary to make this reply timely filed, the Applicant petitions for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Date: May 2, 2005


Craig G. Holmes
Reg. No. 44,770

2055 Gateway Place, Suite 550
San Jose, CA 95110-1089
Telephone: (408) 414-1207
Facsimile: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Hon. Commissioner for Patents, Mail Stop RCE, P.O. Box 1450, Alexandria, VA 22313-1450

on 5/2/05 by Trudy Bagdon
Trudy Bagdon